

#4

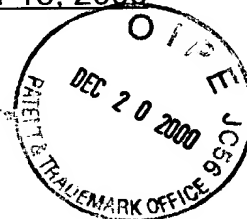
Docket No.: GR 98 P 1180 P

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By: 

Date: December 15, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Applicant : Erwin Hess et al.
Appl. No. : 09/641,868
Filed : August 18, 2000
Title : Method and Device for Cryptographic Processing with the Aid of an Elliptic Curve on a Computer

CLAIM FOR PRIORITY

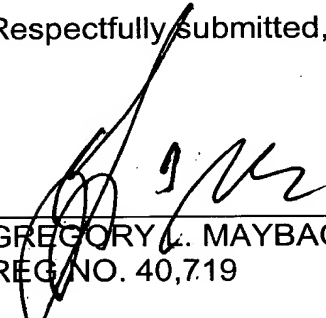
Hon. Commissioner of Patents and Trademarks,
Washington, D.C. 20231

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 198 06 825.5 filed February 18, 1998.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,


GREGORY L. MAYBACK
REG NO. 40,719

Date: December 15, 2000

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/mjb



**Prioritätsbescheinigung über die Einreichung
einer Patentanmeldung**

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

Aktenzeichen: 198 06 825.5

Anmeldetag: 18. Februar 1998

Anmelder/Inhaber: Siemens AG, München/DE

Bezeichnung: Verfahren und Vorrichtung zur kryptographischen
Bearbeitung anhand einer elliptischen Kurve auf
einem Rechner

IPC: G 06 F 17/10

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 19. September 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Nietzsch

Beschreibung**Verfahren und Vorrichtung zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner**

5

Die Erfindung betrifft ein Verfahren und eine Anordnung zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner.

10 Ein endlicher Körper heißt Galois-Feld. Zu den Eigenschaften und zur Definition des Galois-Feldes sei auf [3] verwiesen.

Mit der weiten Verbreitung von Computernetzen und zugehörigen Anwendungen, die über elektronische Kommunikationssysteme

15 (Kommunikationsnetze) abgewickelt werden, werden zunehmend wachsende Anforderungen an die Datensicherheit gestellt. Der Aspekt der Datensicherheit berücksichtigt u.a.

- die Möglichkeit eines Ausfalls der Datenübertragung,
- die Möglichkeit korumpierter Daten,

20 - die Authentizität der Daten, also die Feststellbarkeit und die Identifikation eines Absenders und
- den Schutz der Vertraulichkeit der Daten.

25

Unter einem "Schlüssel" werden Daten verstanden, die bei der kryptographischen Bearbeitung Verwendung finden. Aus Public-Key-Verfahren [4] ist bekannt, einen geheimen und einen öffentlichen Schlüssel einzusetzen.

Ein "Angreifer" ist eine nichtautorisierte Person mit dem
30 Ziel, an den Schlüssel zu gelangen.

Insbesondere in einem Rechnernetz, in zunehmenden Maße aber auch in portablen Medien, z.B. einem Mobiltelefon oder einer Chipkarte, ist sicherzustellen, daß ein abgespeicherter
35 Schlüssel auch dann nicht zugänglich ist, wenn ein Angreifer sich des Rechners, des Mobiltelefons oder der Chipkarte bemächtigt.

Um ausreichende Sicherheit kryptographischer Verfahren zu gewährleisten, werden Schlüssel, insbesondere bei asymmetrischen Verfahren, jeweils mit Längen von mehreren 100
5 Bits bestimmt. Ein Speicherbereich eines Rechners oder portablen Mediums ist zumeist knapp bemessen. Eine Länge eines in einem solchen Speicherbereich abgelegten Schlüssels von mehreren 100 Bits verringert den freien Speicherplatz auf dem Rechner bzw. dem Medium, so daß nur wenige solcher
10 Schlüssel auf einmal abgespeichert werden können.

Aus [1] und [2] ist eine elliptische Kurve und deren Anwendung bei der kryptographischen Bearbeitung bekannt.

15 Die **Aufgabe** der Erfindung besteht darin, ein Verfahren zur kryptographischen Bearbeitung anhand mindestens einer elliptischen Kurve auf einem Rechner anzugeben, wobei weniger Speicherplatz benötigt wird.

20 Diese Aufgabe wird gemäß der Merkmale der unabhängigen Patentansprüche gelöst.

Es wird ein Verfahren zur kryptographischen Bearbeitung anhand mindestens einer elliptischen Kurve auf einem Rechner
25 angegeben, bei dem die elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve in der ersten Form bestimmen. Die elliptische Kurve wird in eine zweite Form transformiert, indem mehrere zweite Parameter bestimmt werden, wobei
30 mindestens einer der zweiten Parameter in seiner Länge gegenüber einem der ersten Parameter verkürzt wird. Die elliptische Kurve nach der Transformation, also in der zweiten Form, wird zur kryptographischen Bearbeitung verwendet.

35

Durch die signifikante Verkürzung eines der ersten Parameter ergibt sich eine Einsparung eines für diesen Parameter

bereitzustellenden Speicherbereichs. Da der Speicherbereich, z.B. auf einer Chipkarte, eng bemessen ist, erreicht man durch die Einsparung mehrerer 100 Bit für jeden verkürzten Parameter freien Speicherplatz z.B. zum Abspeichern eines weiteren geheimen Schlüssels. Durch die Verkürzung des jeweiligen Parameters bleibt die Sicherheit des kryptographischen Verfahrens trotzdem gewährleistet.

Bei Verwendung einer elliptischen Kurve in einem kryptographischen Verfahren steigt der Aufwand für einen Angreifer, den Schlüssel zu ermitteln, exponentiell mit dessen Länge.

Eine Weiterbildung der Erfindung besteht darin, daß die erste Form der elliptischen Kurve bestimmt ist durch:

$$y^2 = x^3 + ax + b \text{ über } GF(p) \quad (1)$$

wobei

$GF(p)$ ein Galois-Feld mit p Elementen und
 x, y, a, b Elemente des Körpers $GF(p)$
bezeichnen.

Die später verwendete Bezeichnung "mod p " bezeichnet einen Spezialfall für das Galois-Feld, nämlich die natürlichen Zahlen kleiner p . "mod" steht für MODULO und umfaßt eine Ganzzahldivision mit Rest.

Eine andere Weiterbildung besteht darin, daß die zweite Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + c^4ax + c^6b \text{ über } GF(p) \quad (2)$$

wobei c eine Konstante bezeichnet.

Zur Einsparung von Speicherplatz wird Gleichung (1) in Gleichung (2) transformiert und eine die elliptische Kurve gemäß Gleichung (2) kennzeichnende Größe verkürzt.

- 5 Eine Weiterbildung besteht darin, den Parameter a zu verkürzen, indem die Konstante c derart gewählt wird, daß

$$c^4 a \bmod p \quad (3)$$

- 10 deutlich kürzer wird als die anderen die elliptische Kurven nach Gleichung (2) beschreibenden Parameter. Durch diese Verkürzung benötigt der Parameter entsprechend weniger Speicherplatz.

- 15 Auch ist es eine Weiterbildung, das Verfahren in einer der folgenden Anwendungen einzusetzen:

- Verschlüsselung bzw. Entschlüsselung:

Daten werden von einem Sender verschlüsselt - mittels symmetrischem oder asymmetrischem Verfahren - und auf der Gegenseite bei einem Empfänger entschlüsselt.

- Schlüsselvergabe durch eine Zertifizierungsinstanz:

Eine vertrauenswürdige Einrichtung (Zertifizierungsinstanz) vergibt den Schlüssel, wobei sichergestellt werden muß, daß der Schlüssel von dieser Zertifizierungsinstanz stammt.

- digitale Signatur bzw. Verifikation der digitalen Signatur:

Ein elektronisches Dokument wird signiert und die Signatur dem Dokument angefügt. Bei dem Empfänger kann anhand der Signatur festgestellt werden, ob auch wirklich der gewünschte Sender unterschrieben hat.

- asymmetrische Authentikation:

Anhand eines asymmetrischen Verfahrens kann ein Benutzer seine Identität nachweisen. Vorzugweise geschieht das durch Codierung mit einem entsprechenden geheimen (privaten) Schlüssel. Mit dem zugehörigen öffentlichen Schlüssel dieses Benutzers kann jeder feststellen, daß die Codierung wirklich von diesem Benutzer stammt.

- Verkürzen von Schlüsseln:

Eine Variante der kryptographischen Bearbeitung umfaßt das Verkürzen eines Schlüssels, welcher Schlüssel bevorzugt für weitergehende Verfahren der Kryptographie verwendet werden kann.

Ferner ist eine Vorrichtung angegeben, die eine Prozessoreinheit aufweist, die derart eingerichtet ist, daß eine elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen, und daß die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber den ersten Parameter verkürzt wird. Schließlich wird die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt.

Diese Vorrichtung kann eine Chipkarte sein, die einen geschützten und einen nicht geschützten Speicherbereich aufweist, wobei sowohl in dem geschützten als auch in dem nichtgeschützten Speicherbereich Schlüssel, also Parameter, die die elliptische Kurve kennzeichnen, abgelegt werden können.

Diese Vorrichtung ist insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner vorstehend erläuterten Weiterbildungen.

Weiterbildungen der Erfindung ergeben sich auch aus den abhängigen Ansprüchen.

Anhand der folgenden Figur werden Ausführungsbeispiele der Erfindung näher dargestellt.

Es zeigen

- Fig.1 ein Verfahren zur kryptographischen Bearbeitung
mittels einer elliptischen Kurve, wobei mindestens
ein Parameter der elliptischen Kurve verkürzt wird
und somit eine Einsparung eines Teils des für die
Parameter der elliptischen Kurve benötigten
Speicherbereichs erfolgt;
- Fig.2 eine Auswahl von Möglichkeiten für die Primzahl p , so
daß der Parameter a der elliptischen Kurve verkürzt
wird;
- Fig.3 ein Verfahren zur Bestimmung einer elliptischen Kurve
und anschließende Transformation in die zweite Form;
- Fig.4 eine Anordnung zur kryptographischen Bearbeitung;
- Fig.5 eine Prozessoreinheit.

Fig.1 zeigt ein Verfahren zur Bearbeitung mittels einer
elliptischen Kurve. Die elliptische Kurve (vgl. Block 101)
wird dazu von einer ersten Form in eine zweite Form
transformiert (vgl. Block 102), ein Parameter der zweiten
Form wird verkürzt (vgl. Block 103) und die zweite Form wird
zur kryptographischen Bearbeitung abgespeichert (vgl. Block
104). Nachfolgend wird auf die genannten Schritte
eingegangen, wobei einige Möglichkeiten für die Verkürzung
beispielhaft herausgegriffen werden.

Es wird beschrieben, wie eine Reduzierung der Länge des
Parameters a in der Gleichung der elliptischen Kurve
(elliptische Kurve in erster Form, siehe Block 101)

$$y^2 = x^3 + ax + b \text{ über } GF(p) \quad (3)$$

erreicht wird, wobei p insbesondere eine Primzahl größer 3
ist und $GF(p)$ ein Galois-Feld mit p Elementen darstellt.

Eine elliptische Kurve

$$y^2 = x^3 + ax + b \text{ über } GF(p) \quad (4)$$

5

läßt sich durch Transformation in eine birational isomorphe elliptische Kurve (elliptische Kurve in zweiter Form, siehe Block 102)

$$y^2 = x^3 + c^4ax + c^6b \text{ über } GF(p) \quad (5)$$

überführen. Durch geeignete Wahl der Konstanten c kann der Koeffizient

$$c^4a \quad \text{bzw.} \quad (6)$$

$$-c^4a \quad (7)$$

verkürzt werden (siehe Block 103) mit dem Vorteil, daß der zur Speicherung dieses Koeffizienten benötigte Speicherplatz im Vergleich zum Speicherplatz für den Parameter a gering sein kann.

Entsprechend Gleichung (5) werden nachfolgend die Zahlen c^4a (bzw. $-c^4a$) und c^2 bestimmt.

1 Bestimmung der Zahl " c^4a "

30

Zur Bestimmung der Zahl c^4a (bzw. $-c^4a$) unterscheidet man bevorzugt die folgenden Fälle:

1.1 $p \equiv 3 \pmod{4}$

35 In diesen Körpern gilt:

- alle Quadrate sind auch vierte Potenzen,

- '-1' ist kein Quadrat.

Es sei nun $p = 4k + 3$ und s eine vierte Potenz, welche die multiplikative Untergruppe der vierten Potenzen (bzw. der Quadrate) in $GF(p)$ erzeugt.

Es ist

$V = \{1, s, s^2, s^3, \dots, s^{2k}\}$ die Menge der vierten Potenzen in $GF(p)$ und

$NQ = \{-1, -s, -s^2, -s^3, \dots, -s^{2k}\}$ die Menge der Nichtquadrate in $GF(p)$.

1. Zu jedem Element $a = s^t$ aus V
 existiert ein Element $c^4 = s^{2k+1-t}$ aus V
 mit $c^4 a = s^{2k+1} = 1$ in $GF(p)$.
2. Zu jedem Element $a = -s^t$ aus V
 existiert ein Element $c^4 = s^{2k+1-t}$ aus V
 mit $c^4 a = -s^{2k+1} = -1$ in $GF(p)$.

Dabei bezeichnen s , t und k Körperelemente aus $GF(p)$.

Für $p \equiv 3 \pmod{4}$ läßt sich der Parameter a durch geeignete Wahl der Konstanten c in die Zahl $c^4 a = 1$ in $GF(p)$ oder $c^4 a = -1$ in $GF(p)$ überführen.

1.2 $p \equiv 1 \pmod{4}$

In einem solchen Körper gilt:

- $(p-1)/4$ Elemente der multiplikativen Gruppe des Körpers sind vierte Potenzen;
- $(p-1)/4$ Elemente der multiplikativen Gruppe des Körpers sind Quadrate, aber keine vierten Potenzen;
- $(p-1)/2$ Elemente der multiplikativen Gruppe des Körpers sind Nichtquadrate;

- '-1' ist kein Nichtquadrat.

A) $p \equiv 5 \pmod{8}$

5

In einem solchen Körper gilt zusätzlich:

- '-1' ist ein Quadrat, aber keine vierte Potenz,
- '+2', '-2' sind Nichtquadrate.

10

Es sei nun $p = 8k + 5$ und s eine vierte Potenz, welche die multiplikative Untergruppe der vierten Potenz in $GF(p)$ erzeugt.

Es ist

15

$$V = \{1, s, s^2, s^3, \dots, s^{2k}\}$$

die Menge der vierten
Potenzen in $GF(p)$ und

$$Q = \{-1, -s, -s^2, -s^3, \dots, -s^{2k}\}$$

die Menge der Quadrate,
die keine vierten Potenzen
in $GF(p)$ sind und

20

$$NQ = \{2, 2s, 2s^2, 2s^3, \dots, 2s^{2k}, -2, -2s, -2s^2, -2s^3, \dots, -2s^{2k}\}$$

die Menge
der Nichtquadrate in
 $GF(p)$.

25

1. Zu jedem Element
existiert ein Element
mit

$$\begin{aligned} a &= s^t \text{ aus } V \\ c^4 &= s^{2k+1-t} \text{ aus } V \\ c^4 a &= s^{2k+1} = 1 \text{ in } GF(p). \end{aligned}$$

30

2. Zu jedem Element
existiert ein Element
mit

$$\begin{aligned} a &= -s^t \text{ aus } Q \\ c^4 &= s^{2k+1-t} \text{ aus } V \\ c^4 a &= -s^{2k+1} = -1 \text{ in } GF(p). \end{aligned}$$

3. Zu jedem Element
existiert ein Element
mit

$$\begin{aligned} a &= 2s^t \text{ aus } NQ \\ c^4 &= s^{2k+1-t} \text{ aus } V \\ c^4 a &= 2s^{2k+1} = 2 \text{ in } GF(p). \end{aligned}$$

35

10

4. Zu jedem Element $a = -2s^t$ aus NQ
 existiert ein Element $c^4 = s^{2k+1-t}$ aus V
 mit $c^4 a = -2s^{2k+1} = -2$ in $GF(p)$.

5 Für $p \equiv 5 \pmod{8}$ läßt sich der Parameter a durch
 geeignete Wahl der Konstanten c in die Zahl
 $c^4 a = 1$ oder -1 oder 2 oder -2 in $GF(p)$
 überführen.

10

B) $p \equiv 1 \pmod{8}$

Die Zahl $c^4 a$ läßt sich nach folgendem Schema ermitteln:

15

- Für $r=1, -1, 2, -2, 3, -3, 4, -4, \dots$
 - bilde $z \equiv ra^{-1} \pmod{p}$;
 - berechne $u \equiv z^{(p-1)/4} \pmod{p}$;
 - abbrechen, falls $u=1$ ist;
 - speichere $z = c^4$ und $r = c^4 a$.

20

2 Bestimmung der Zahl " c^2 in $GF(p)$ "

Zur Bestimmung der Zahl $c^2 \pmod{p}$ wird zunächst im
 25 entsprechenden Körper $GF(p)$ festgestellt, ob a eine vierte
 Potenz, ein Quadrat aber keine vierte Potenz oder ein
 Nichtquadrat ist.

2.1 $p = 4k + 3$

30

- In diesen Körpern wird $u = a^{(p-1)/2}$ in $GF(p)$ berechnet.
 - Ist $u=1$ in $GF(p)$, so ist a eine vierte Potenz (bzw.
 ein Quadrat). In diesem Fall ist $c^4 = a^{-1}$ in $GF(p)$.
 - Ist $u=-1$ in $GF(p)$, so ist a ein Nichtquadrat. In
 diesem Fall ist $c^4 = -a^{-1}$ in $GF(p)$.

35

2.2 $p = 8k + 5$

11

In diesen Körpern wird $u = a^{(p-1)/4}$ in $GF(p)$ berechnet.

- Ist $u=1$ in $GF(p)$, so ist a eine vierte Potenz. In diesem Fall ist $c^4 = a^{-1}$ in $GF(p)$.

5 - Ist $u=-1$, so ist a ein Quadrat aber keine vierte Potenz. In diesem Fall ist $c^4 = -a^{-1}$ in $GF(p)$.

- Ist u weder 1 noch -1 in $GF(p)$, so ist a ein Nichtquadrat in $GF(p)$. In diesem Fall wird $v = (2a)^{(p-1)/4}$ in $GF(p)$ berechnet. Ist $v=1$ in $GF(p)$, so ist $c^4 = 2a^{-1}$ in $GF(p)$, sonst ist $c^4 = -2a^{-1}$ in $GF(p)$.

10

2.2 $p = 8k + 1$

In diesen Körpern ist nach dem in 1.2, Fall B beschriebenen Schema $z = c^4$.

15

In allen drei Fällen lassen sich mit einem Aufwand von $O(\log p)$ die beiden Wurzeln (c^2 und $-c^2$) aus c^4 berechnen. Für den Fall $p = 4k + 3$ ist nur eine der beiden angegebenen Lösungen zulässig, nämlich diejenige, die ein Quadrat in $GF(p)$ ist. In den anderen Fällen sind beide Lösungen
20 zulässig. Somit läßt sich der Koeffizient c^6_b der elliptischen Kurve berechnen.

Aufgrund der geschlossenen Formeln für die Fälle $p = 4k + 3$
25 und $p = 8k + 5$ sind in der Praxis derartige Primzahlen zu bevorzugen.

Beispiel 1:

Es sei die Primzahl $p = 11 \Rightarrow$ Fall 1.1: $p \equiv 3 \pmod{4}$

Zahl	Quadrate Q	vierte Potenzen V
1	1	1
2	4	5
3	9	4
4	5	3
5	3	9
6	3	9
7	5	3
8	9	4
9	4	5
10	1	1

5 Tabelle 1: Quadrate und vierte Potenzen mod 11

Damit ergeben sich die Menge der Quadrate Q, die Menge der vierten Potenzen V und die Menge der Nichtquadrate NQ zu:

$$Q = V = \{1, 3, 4, 5, 9\};$$

10 $NQ = \{2, 6, 7, 8, 10\}.$

$$\underline{a \in V = Q} \quad \Rightarrow \quad ac^4 = 1$$

a=	$c^4=$
1	1
3	4
4	3
5	9
9	5

Tabelle 2: Bestimmung von c^4 bei gegebenem Parameter a

13

$$\underline{a \in \mathbb{N}_Q} \Rightarrow ac^4 = -1$$

a=	c ⁴ =
2	5
6	9
7	3
8	4
10	1

Tabelle 3: Bestimmung von c^4 bei gegebenem Parameter a

5 Tabelle 2 zeigt verschiedene Möglichkeiten einer Wertzuordnung von a und c^4 auf, die in der Verknüpfung ac^4 stets 1 ergeben, und Tabelle 3 zeigt verschiedene Möglichkeiten einer Wertzuordnung von a und c^4 auf, die in der Verknüpfung ac^4 stets -1 ergeben. Dies gilt in $\text{GF}(11)$.

10

Beispiel 2:

Es sei die Primzahl $p = 13 \Rightarrow \text{Fall 1.2 A): } p \equiv 1 \pmod{4} \text{ und zugleich } p \equiv 5 \pmod{8}$.

15

Zahl	Quadrate Q	vierte Potenzen V
1	1	1
2	4	3
3	9	3
4	3	9
5	12	1
6	10	9
7	10	9
8	12	1
9	3	9
10	9	3
11	4	3
12	1	1

Tabelle 4: Quadrate und vierte Potenzen mod 13

Damit ergeben sich die Menge der Quadrate Q (die keine vierten Potenzen sind), die Menge der vierten Potenzen V und die Menge der Nichtquadrate NQ zu:

$$Q = \{4, 10, 12\};$$

$$5 \quad V = \{1, 3, 9\};$$

$$NQ = \{2, 5, 6, 7, 8, 11\}.$$

$$\underline{a \in V} \quad \Rightarrow \quad c^4 \in V$$

a=	$c^4 =$
1	1
3	9
9	3

10 Tabelle 5: Bestimmung von c^4 bei gegebenem Parameter a

$$\Rightarrow ac^4 \equiv 1 \pmod{13}$$

$$15 \quad \underline{a \in Q}$$

a=	$c^4 =$	$ac^4 =$
4	3	$12 \equiv -1 \pmod{13}$
10	9	$90 \equiv -1 \pmod{13}$
12	1	$12 \equiv -1 \pmod{13}$

Tabelle 6: Bestimmung von c^4 bei gegebenem Parameter a

$$\Rightarrow ac^4 \equiv -1 \pmod{13}$$

20

$$\underline{a \in NQ}$$

$$NQ = \{2, 5, 6, 7, 8, 11\}, \text{ mit}$$

$$25 \quad 2 \cdot V = \{1, 5, 6\} \text{ und}$$

$$2 \cdot Q = \{7, 8, 11\}$$

$$\underline{\text{Fall } a: a \in NQ \text{ und } a \in (2 \cdot V)}$$

a=	$c^4 =$	$ac^4 =$
2	1	$2 = 2 \bmod 13$
5	3	$15 = 2 \bmod 13$
6	9	$54 = 2 \bmod 13$

Tabelle 7: Bestimmung von c^4 bei gegebenem Parameter a

$$\Rightarrow ac^4 \equiv 2 \bmod 13$$

5

Fall b: $a \in \mathbb{N}\mathbb{Q}$ und $a \in (2 * \mathbb{Q})$

a=	$c^4 =$	$ac^4 =$
7	9	$63 = -2 \bmod 13$
8	3	$24 = -2 \bmod 13$
11	1	$11 = -2 \bmod 13$

Tabelle 8: Bestimmung von c^4 bei gegebenem Parameter a

$$\Rightarrow ac^4 \equiv -2 \bmod 13$$

10

Die auf die beschriebene Art gewonnene elliptische Kurve in der zweiten Form (siehe Block 103) wird zu einer

15

Fig.2 zeigt eine Auswahl von Möglichkeiten für die Wahl der Primzahl p zur Verkürzung des Parameters a (siehe Block 201), wie oben beschrieben. Die Möglichkeit 202 bestimmt p derart, daß $p = 3 \bmod 4$ gilt. In diesem Fall läßt sich der Parameter a anhand oben beschriebener Vorgehensweise verkürzen. Das gleiche gilt für $p = 1 \bmod 4$ (Fall 203), wobei eine Fallunterscheidung gesondert die beiden Fälle $p = 5 \bmod 8$ (Fall 204) und $p = 1 \bmod 8$ (Fall 205) anführt. Die geschlossenen Formulierungen zur Bestimmung eines verkürzten Parameters a sind jeweils oben ausgeführt. Fig.2 zeigt ausdrücklich eine Auswahl von Möglichkeiten auf, ohne einen Anspruch auf eine umfassende Auswahl anzustreben.

20

25

In Fig.3 wird in einem ersten Schritt 301 eine elliptische Kurve mit den Parametern a , b , p und einer Punktezahl ZP gemäß Gleichung (1) bestimmt. In einem Schritt 302 wird die
5 elliptische Kurve transformiert (vgl. Gleichung (2)). Nach der Transformation umfaßt die elliptische Kurve die Parameter a' , b' , p und ZP . a' und b' deuten an, daß die Parameter a und b verändert wurden, wobei ein Parameter, vorzugsweise der Parameter a' kurz ist im Vergleich zu dem Parameter a , so daß
10 durch Abspeichern des Parameters a' anstelle des Parameters a als Kennzeichen der elliptischen Kurve Speicherplatz eingespart wird.

In Fig.4 ist eine Anordnung zur kryptographischen Bearbeitung
15 dargestellt.

Ein portables Medium 401, vorzugsweise eine Chipkarte, umfaßt einen (unsicheren) Speicherbereich MEM 403 und einen geschützten (sicheren) Speicherbereich SEC 402. Anhand einer
20 Schnittstelle IFC 404 werden über einen Kanal 405 Daten zwischen dem Medium 401 und einem Rechnernetz 406 ausgetauscht. Das Rechnernetz 406 umfaßt mehrere Rechner, die miteinander verbunden sind und untereinander kommunizieren. Daten für den Betrieb des portablen Mediums 401 sind
25 vorzugsweise in dem Rechnernetz RN 406 verteilt verfügbar.

Der geschützte Speicherbereich 402 ist nicht lesbar ausgeführt. Anhand einer Recheneinheit, die auf dem portablen Medium 401 oder im Rechnernetz 406 untergebracht ist, werden
30 die Daten des geschützte Speicherbereichs 402 genutzt. So kann eine Vergleichsoperation als Ergebnis angeben, ob ein Vergleich einer Eingabe mit einem Schlüssel im geschützte Speicherbereich 402 erfolgreich war oder nicht.

35 Die Parameter der elliptischen Kurve sind in dem geschützten Speicherbereich 402 oder in dem ungeschützten Speicherbereich 403 abgelegt. Insbesondere wird ein geheimer oder privater

Schlüssel in dem geschützten Speicherbereich und ein öffentlicher Schlüssel in dem unsicheren Speicherbereich abgespeichert.

- 5 In Fig.5 ist eine Recheneinheit 501 dargestellt. Die Recheneinheit 501 umfaßt einen Prozessor CPU 502, einen Speicher 503 und eine Input/Output-Schnittstelle 504, die über ein aus der Recheneinheit 501 herausgeführtes Interface 505 auf unterschiedliche Art und Weise genutzt wird: Über
- 10 eine Grafikschnittstelle wird eine Ausgabe auf einem Monitor 507 sichtbar und/oder auf einem Drucker 508 ausgegeben. Eine Eingabe erfolgt über eine Maus 509 oder eine Tastatur 510. Auch verfügt die Recheneinheit 501 über einen Bus 506, der die Verbindung von Speicher 503, Prozessor 502 und
- 15 Input/Output-Schnittstelle 504 sicherstellt. Weiterhin ist es möglich, an den Bus 506 zusätzliche Komponenten anzuschließen: zusätzlicher Speicher, Festplatte, etc.

Literaturverzeichnis:

[1] Neal Koblitz: A Course in Number Theory and Cryptography,
Springer Verlag New York, 1987, ISBN 0-387-96576-9,
Seiten 150-179.

5 [2] Alfred J. Menezes: Elliptic Curve Public Key
Cryptosystems, Kluwer Academic Publishers, Massachusetts
1993, ISBN 0-7923-9368-6, Seiten 83-116.

[3] Rudolf Lidl, Harald Niederreiter: Introduction to finite
fields and their applications, Cambridge University
10 Press, Cambridge 1986, ISBN 0-521-30706-6, Seiten 15, 45.

[4] Christoph Ruland: Informationssicherheit in Datennetzen,
DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3,
Seiten 73-85.

Patentansprüche

1. Verfahren zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner,
- 5 a) bei dem die elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen,
- 10 b) bei dem die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber dem ersten Parameter verkürzt wird.
- c) bei dem die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt wird.
- 15 2. Verfahren nach dem vorhergehenden Anspruch, bei dem die erste Form der elliptischen Kurve bestimmt ist durch

20
$$y^2 = x^3 + ax + b,$$

wobei

x, y Variablen und
a, b die ersten Parameter

35 bezeichnen.

3. Verfahren nach Anspruch 1 oder 2, bei dem die zweite Form der elliptischen Kurve bestimmt ist durch

30
$$y^2 = x^3 + c^4 ax + c^6 b,$$

wobei

x, y Variablen,
a, b die ersten Parameter und
35 c eine Konstante

bezeichnen.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem der Parameter a verkürzt wird, indem die
Konstante c derart gewählt wird, daß

5

$$c^4 a \bmod p$$

deutlich kürzer bestimmt wird als die Längen des
Parameters b und die Länge der vorgegebenen Größe p.

10

5. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem eine kryptographische Verschlüsselung
durchgeführt wird.

15

6. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem eine kryptographische Entschlüsselung
durchgeführt wird.

20

7. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem eine Schlüsselvergabe durchgeführt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem eine digitale Signatur durchgeführt wird.

25

9. Verfahren nach Anspruch 8,
bei dem eine Verifikation der digitalen Signatur
durchgeführt wird.

30

10. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem eine asymmetrische Authentikation durchgeführt
wird.

35

11. Vorrichtung zur kryptographischen Bearbeitung,
mit eineressoreinheit, die derart eingerichtet ist,
daß

- a) eine elliptische Kurve in einer ersten Form vorgegeben wird, wobei mehrere erste Parameter die elliptische Kurve bestimmen,
- b) die elliptische Kurve in eine zweite Form transformiert wird, indem mehrere zweite Parameter bestimmt werden, wobei mindestens einer der zweiten Parameter in seiner Länge gegenüber den ersten Parameter verkürzt wird.
- c) die elliptische Kurve in der zweiten Form zur kryptographischen Bearbeitung bestimmt wird.

12. Vorrichtung nach Anspruch 11,
bei der die Prozessoreinheit derart eingerichtet ist, daß die erste Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + ax + b,$$

wobei

x, y Variablen und
a, b die ersten Parameter

bezeichnen.

13. Vorrichtung nach Anspruch 11 oder 12,
bei der die Prozessoreinheit derart eingerichtet ist, daß die zweite Form der elliptischen Kurve bestimmt ist durch

$$y^2 = x^3 + c^4ax + c^6b,$$

wobei

x, y Variablen,
a, b die ersten Parameter und
c eine Konstante

bezeichnen.

14. Vorrichtung nach einem der Ansprüche 11 bis 13,
bei der die Prozessoreinheit derart eingerichtet ist, daß

der Parameter a verkürzt wird, indem die Konstante c derart gewählt wird, daß

$$c^4 a \bmod p$$

5

deutlich kürzer bestimmt wird als die Längen des Parameters b und die Länge der vorgegebenen Größe p .

10

15. Vorrichtung nach einem der Ansprüche 11 bis 14,
bei der die Vorrichtung eine Chipkarte mit einem Speicherbereich ist, wobei in dem Speicherbereich die Parameter der elliptischen Kurve abspeicherbar sind..

15

16. Vorrichtung nach Anspruch 15,
bei dem ein geheimer Schlüssel in einem geschützten Speicherbereich der Chipkarte abspeicherbar ist.

Zusammenfassung

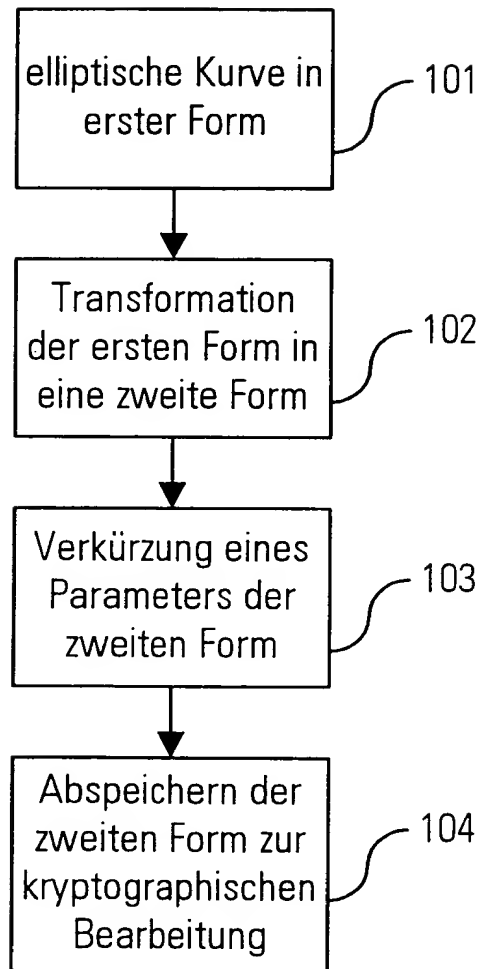
Verfahren und Vorrichtung zur kryptographischen Bearbeitung anhand einer elliptischen Kurve auf einem Rechner

5

Bei der kryptographischen Bearbeitung anhand einer elliptischen Kurve werden Parameter der elliptischen Kurve in einem Speicher eines Rechners abgespeichert. Diese Parameter weisen jeweils erhebliche Länge auf. Um mindestens einen
10 Parameter in seiner Länge deutlich zu verkürzen und dabei unverändert hohe Sicherheit zu gewährleisten, wird die elliptische Kurve transformiert. Mit einem Algorithmus wird ein Parameter bevorzugt zu 1, -1, 2 oder -2 verkürzt, wohingegen die anderen Parameter mehrere 100-Bit Länge
15 aufweisen. Gerade bei Chipkarten, die wenige Speicherplatz aufweisen, macht sich die Verkürzung schon eines Parameters deutlich bemerkbar.

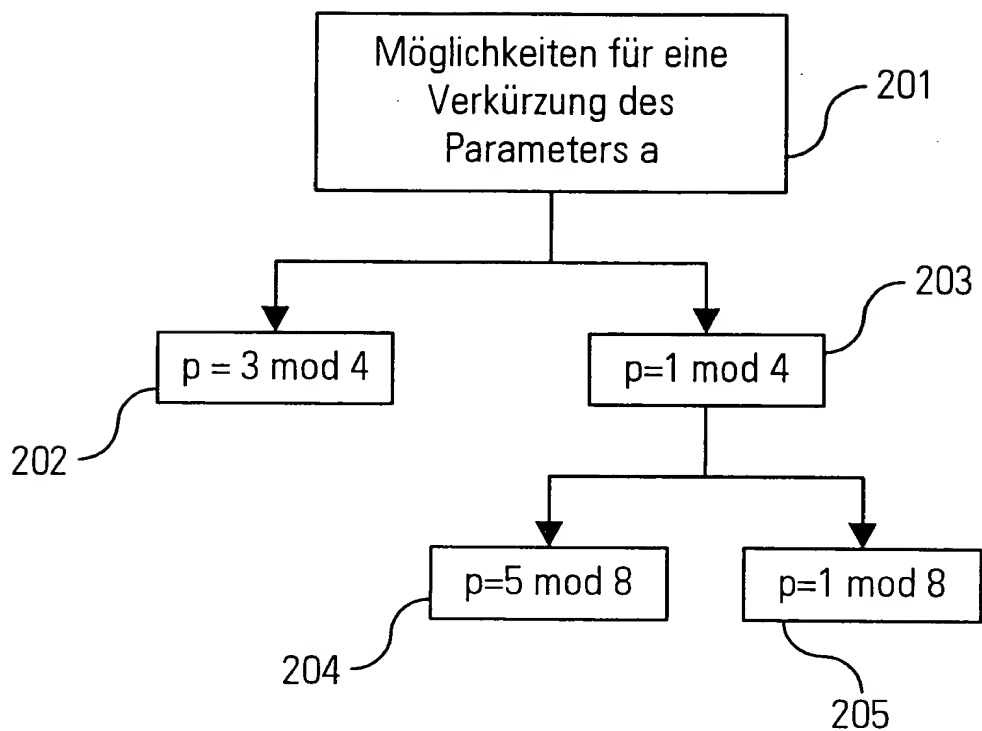
1/4

FIG 1



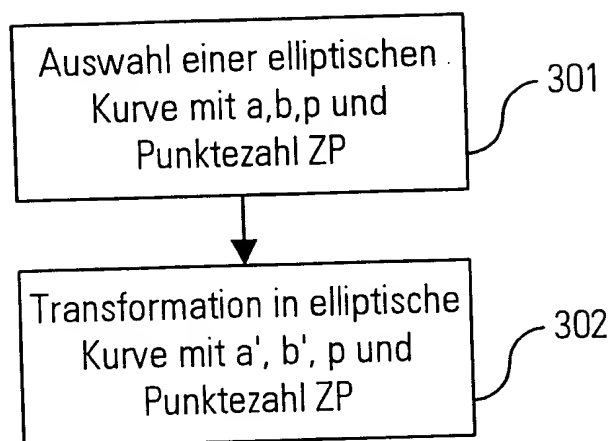
2/4

FIG 2



3/4

FIG 3



4/4

FIG 4

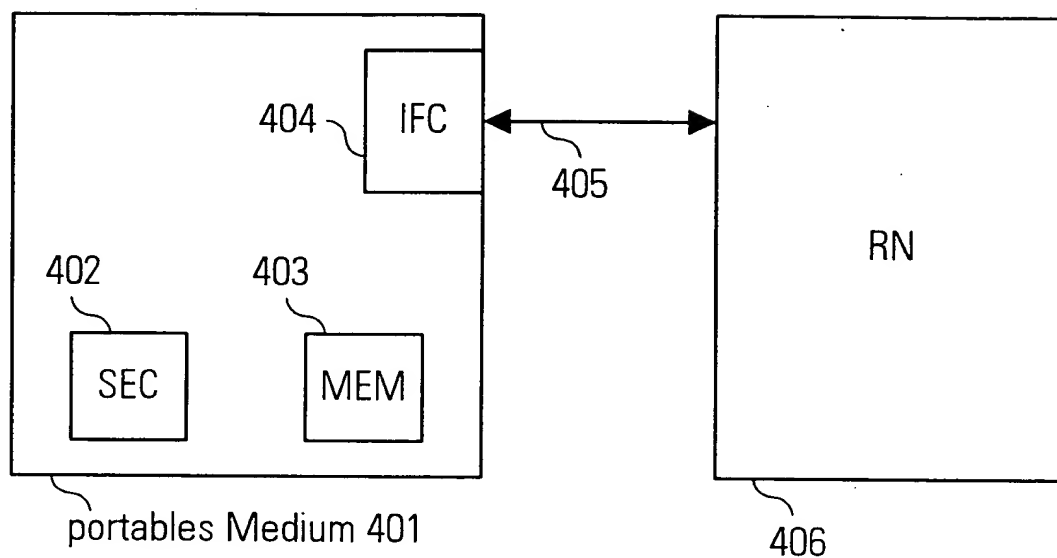


FIG 5

